⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−185585

⑤Int.Cl.[5]	識別記号	庁内整理番号	㊸公開　平成3年(1991)8月13日
G 06 K 17/00	S	6711−5B	
G 07 F 7/12			
H 04 N 7/18	K	7033−5C	
		8208−3E　G 07 F 7/08	C

審査請求　未請求　請求項の数 5　(全10頁)

㊹発明の名称　ＩＤカードの真偽判別方式及び真偽判別装置

㉑特　願　平1−323925
㉒出　願　平1(1989)12月15日

㉒発明者　永戸　一志　神奈川県川崎市幸区小向東芝町1番地　株式会社東芝総合研究所内
㉑出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地
㉔代理人　弁理士　則近　憲佑　外1名

明　細　書

1．発明の名称

ＩＤカードの真偽判別方式及び真偽判別装置

2．特許請求の範囲

(1) パーソナルデータ、および写真データを、ドットプリンタで記録し、作成するＩＤカードに於て、少なくとも写真データ部の画点の主走査方向又は副走査方向の画点の濃度変化を調べ、この周期が、写真データを記録したプリンタの解像度と一致した場合には、真のＩＤカードであり、一致しない場合には、偽のＩＤカードであると判別する、ＩＤカードの真偽判別方式。

(2) 解像度が、ＩＤカードを作成したプリンタの最小解像度より、更に細かく解像できる性能を持った、光検出器を持つことを特徴とする請求項1記載のＩＤカードの真偽判別方式を使用した、ＩＤカード真偽判別装置。

(3) 少なくとも写真データを昇華性染料を使用した、いわゆる熱昇華記録によって形成したＩＤカードの場合には、近赤外光と、近赤外光に反応して出力を生ずる光検出器の組合わせにより、写真データ部での反射光がほぼ一様でない場合には、偽のＩＤカードであると判別するＩＤカードの真偽判別方式。

(4) ＩＤカードの様々な部分を解像度の異なるいくつかのプリンタで記録し、ＩＤカードを読み取った場合に、それぞれの部分が、それぞれのプリンタの解像度と一致しているかを調べ、少なくとも一箇所以上で一致が得られている場合にそのＩＤカードは偽物でない可能性があると判断するＩＤカードの真偽判別方式。

(5) パーソナルデータを特別な変換式に基づいて変換し、写真データ部に、この変換に基づいた結果を記録しておき、ＩＤカードのパーソナルデータを読み取った場合に、予めわかっている変換式に基づいて変換し、そのデータと写真部から読み取ったデータが一致していることによって、真のＩＤカードであると判別するＩＤカードの真偽判別方式。

3．発明の詳細な説明

［発明の目的］

（産業上の利用分野）

この発明は、文字化されたパーソナルデータと、本人の顔写真が記録されたＩＤカードに於て、パーソナルデータが顔写真で示されている人物であるか否かを判定するＩＤカードの真偽判別方式及び真偽判別装置に関する。

（従来の技術）

従来ＩＤカードは、パーソナルデータが印刷された紙あるいはプラスチック上に、顔写真などを合わせ、これらを一括して、ラミネートすることによって形成していた。ＩＤカードは、社員証，クレジットカード，ＣＤカード，あるいは個人を証明するカードとして使用されている。ＩＤカード内にはパーソナルデータとして、本人の名前，生年月日，個人番号（社員証なら、社員番号など…）更に、ＩＤカードの発行ナンバーなどが記録されている。これらのパーソナルデータは、可視化されているものもあるが、場合によっては磁気カードのような不可視な状態で記録されているものもある。

従来、ＩＤカードの使用量は、あまり多くなかったが、最近では様々な分野に於て、ＩＤカードが使用されるようになってきた。しかし、これと同時にこれらのカードに関する不正使用も多発するようになってきている。例えばカードのパスワード、暗証番号などを調べだし、他人のカードを不正に使用することなとが行なわれている。

（発明が解決しようとする課題）

ＩＤカードには、パーソナルデータが記録されている他に、本人の顔写真が記録されている。従って、カードと本人を見比べることによって、本人が自分自身のＩＤカードを使用していることが確認できる。（なお、今後全ての場合、記録されているパーソナルデータは正しいのであると仮定した上で話を行っていく。従って、ＩＤカードに貼られてある写真と、本人の顔が一致していればＩＤカードに記録されたパーソナルデータも、本人のものであるとする。）このようなＩＤカードを使用する場合に、他人のＩＤカードを使用し、顔写真だけ自分のものと貼りかえる偽造を行なう、例えば第１０図(a)の顔写真部分を切り取り、(b)のように他人の写真を入れることによって、他人のパーソナルデータを悪用することが可能となる。例えばこのＩＤカードを出退勤務システムに利用している会社があるとすると、この偽造したＩＤカードで他社内部まで浸入でき、重要な機密情報を持ち出すことなどが可能となる。パーソナルデータの偽造については、パーソナルデータが数字，アルファベットなどで構成されているために、これらの数字や文字に特殊な変換をほどこし、チェックコードなどをつくり出し、パーソナルデータ中に合わせて入れておくため、偽造はむずかしい。しかし、顔写真については、他人の顔写真と貼り変える方法あるいは他人の顔写真を貼った、ＩＤカードを写真で取ってしまう方法などによって、簡単に偽造できてしまう。本発明の目的は、ＩＤカードのパーソナルデータと、そこに記録されている本人の顔写真が正しいものであるかを判断する方法について示すことを本発明の目的としている。

［発明の構成］

（課題を解決するための手段）

上述した問題的を解決するために、本発明のＩＤカードの読み取り方式は、パーソナルデータを読み取る手段と、更に写真部にも記録されているデータを読みと取る手段とを持っていることを特徴としており、これらの間のデータの関係が、規定通りのものであるかどうかを調べ、ＩＤカードの真偽を調べる方式である。

（作　用）

このような構成に成っているために、読み取ったパーソナルデータあるいはこのデータの一部又は、このパーソナルデータをある一定の変換式に基づいて、得られたデータなどと、写真部から読み取ったデータとを比較することにより、これらが一致した場合には、このＩＤカードは正しいカードであるとし、不一致を生じた場合には偽造ＩＤカードであると判別可能となる。

（実施例）

・第１の実施例

以下図面を参照し、本発明の実施例について幾つか示す。まず、本発明で使用するＩＤカードでは、個人によって異なるデータ、つまりパーソナルデータや顔写真のデータは全てプリンタで記録することを前提とする。他の共通部分は、予め印刷で記録してあっても、個人データを記録する際にプリンタで同時に記録してもかまわない。第１０図(a)にＩＤカードの代表例を示す。このＩＤカードでは、パーソナルデータと顔写真で構成されている。まず最も簡単に考えられる偽造法は顔写真の部分を切り取り、又はその上に他人の顔写真を貼りつけ再度写真にとって、行う方法である（第１０図(b)）。このようなＩＤカードを使用しても、通常のチェッカーでは、パーソナルデータ部しかチェックしてないために、本ものと判定してしまう。これを防止する方法を次に示す。

まず最も基本的なチェックの方法としては、顔写真部のチェックも同時に行なって、少なくとも、この顔の部分が後からはめ込まれた合成写真でないことをチェックする方法である。この方法としては、チェッカー内のセンサで顔写真部を読み取り、プリンタで記録されたものか、写真がはめ込まれたものであるかを判定する方法である。幸いなことに本ＩＤカードは解像度の一定なプリンタで記録されているために、拡大してみると各画点がはっきりと認識できる。つまりプリンタの解像度は８ドット／㎜～１６ドット／㎜程度であるので、約１２５μｍ～62.5μｍ程度の画点が見えるはずである（第１図(a)に示すように）。これに対し、顔写真の部分が写真で記録されている場合には、これに対し、写真の銀粒子は１μｍ以下の小さな粒子である。従って顔写真部をセンサでチェックした場合に、プリンタの解像度に相当する画点が見えず、濃度が連続的に変化しているようであれば、（第１図(b)に示すように）ほぼ写真を使用したものであると考えられ、偽造ＩＤカードであると考えられることができる。

なお、ＩＤカードに他人の顔写真を貼って、全体を写真にとって、偽造ＩＤカードを作る場合もあるので、顔写真ばかりでなく、他のパーソナルデータの部分も、センサでスキャンすることにより規定どおりの解像度の画点が観測できるか、否かによってＩＤカード全体が写真で偽造されたかの判定を行うことが可能となる。

・第２の実施例

ＩＤカードの顔写真が他人の顔写真と入れ換えられた場合に偽造ＩＤカードと、判定する第２の実施例を示す。顔写真の部分は階調性を、重視しているために、昇華性のカラーインクを使用した、熱記録装置が、多く使用されている。本発明に使用しているＩＤカードは、熱昇華性インクを使用したカラープリンタで顔写真部を記録しているものとする。第２図にマゼンタインクの反射率を示す。熱昇華性インクは近赤外光に対しては、ほとんど透明である。昇華性インクには染料が使用されており、近赤外光に対しては透明だからである。従って、顔写真の部分を、近赤外光で、走査しても、センサではほとんど反射光は一様となってしまう。なお、パーソナルデータの部分は、顔料を主体としたインクが使用されているために、近赤外光でも充分な吸収があるために、パーソナルデータを読み取り可能である。これに対し、写真などを顔の部分に入れ込んで、偽造したＩＤカードでは、写真部の銀が、近赤外光に対しても、充分な反射特性を持っているために、顔写真の部分を赤外光で走査すると信号が検出できる。つまり、顔写真の部分に写真を使用した場合と、熱昇華性インクを使用した場合とで、近赤外光を当てた時の反射率が全く異なっていることから、ＩＤカードの真偽が判定できるのである。

・第３の実施例

第２の実施例では、顔写真の部分のインクの特性と、パーソナルデータ部を記録したインクの特性の違いを考慮することによって、ＩＤカードの真偽を判定する方法を示したが、本実施例もこの実施例に似た方式である。例えば顔写真の部分を記録した後に、更に特殊なパターンを、紫外光を当てると可視光を発する様なけい光印刷によって印刷する方法もある。第３図にはけい光イ

ンクを説明してある。横軸は波長たて軸は吸収又は発光強度を表わしている。けい光インクのあるものは、第3図のように紫外光を吸収し可視光をけい光として発している。なお図で破線で示すように、赤外域にけい光を発するインクもある。このようなインクを使用すると可視光領域では全く見えなくなることも可能である。ＩＤカードのチェッカでは、紫外光を当てて、例えば可視光のけい光パターンを読み取り、定められた位置に定められたパターンが記録されていることを確かめることで、このＩＤカードの真偽をチェックすることができる。更にこの場合にも第1の実施例などといっしょに使用し、このけい光パターンも一定の解像度のプリンタで記録されたことを、チェックすることによって、更にＩＤカードの真偽性を充分に確認することが可能となる。

なお、けい光記録を行った場合には特殊な機械を使用しなくても、紫外線の下で見ることによって、ある程度の判定は可能である。つまり、特殊なけい光パターンが見える場合にはある程度、本物である可能性が高い。しかし、けい光印刷で偽造した可能性もあるので、チェッカによって、規定の解像度の画点が形成されているか確認する必要がある。

・第4の実施例

今までの実施例で述べた方法では写真を使用して、偽造を行う方法であるが、ＩＤカードもプリンタで作成したものであるので、当然のことながらプリンタを使用しての偽造も考えられないことはない。このような場合には、まず偽造をしにくくする方法として、パーソナルデータ部を記録するプリンタと、顔写真を記録するプリンタの解像度を変えておく方法がある。当然プリンタを使用して、偽造したＩＤカードであるので、第1の実施例で示した方法で偽造を確認しようとしても、プリンタで記録した画点が見えるので、当然本ものと判定してしまう。

そこで、例えばパーソナルデータ部のプリンタの解像度と、顔写真記録用プリンタの解像度を変化させておき、ＩＤカードチェッカーのセンサで、それぞれの部分を読み取った場合に、生ずる1つの画点の大きさの違いから真偽を判定するのが、本発明の第2の実施例である。例えば、第4図の示す様にパーソナルデータ部が10ドット／㎜のプリンタで記録されているとすると、約100μ程度の画点が記録でき、また顔写真が12ドット／㎜のプリンタで記録されているとすると、約82.5μ程度の画点が記録されることになる。従ってこのようにパーソナルデータ部と、顔写真部記録用のプリンタの解像度を変化させてある場合には、パーソナルデータ部と顔写真部をセンサでチェックした場合に、同じ大きさの画点で記録されているとなると、偽造ＩＤカードであると判定できる。

なお、この実施例では、パーソナルデータ部用プリンタ，顔写真記録用プリンタと、解像度の異なる2台のプリンタを使用しているが、より偽造防止を考えるためには、より多数，多種類の、プリンタを使用して、それぞれの解像度を変えておくことによって、偽造防止の効果を大きくすることができる。

・第5の実施例

以上の実施例ではＩＤカード作成機と全く同様の解像度を持ったプリンタ，同じ特性を持ったインクなどが、用意できなかった場合が全て前提となっているか、これらが用意できれば基本的には本物と同じＩＤカード発行器を構成できるはずである。この様な場合に、ＩＤカードの真偽を判定する方法、すなわちパーソナルデータと顔写真の人物との一致を判定する方法としては、基本的には顔写真の中にも、パーソナルデータ又はこの一部あるいは、パーソナルデータより作成されるデータが記録されている必要がある。

1例をあげると、第5図(a)に示すように写真データの中に、パーソナルデータより作成されるデータを記録する方法である。もちろん、このデータの生成方法は、パーソナルデータから第5図(b)のように作成し、ＩＤカードの製作者以外は知らないので適当な数にすることはできない。つまり、パーソナルデータと写真中の文字を比較

するとによって、ＩＤカードの真偽の判定が可能となるわけである。ただし、もちろん、現在の写真技術や、プリント技術を用いることによって、他人の写真を使用し、この写真の中に同一の文字を記録して、偽造してしまう方法もある。写真技術で作った場合には第１の実施例を使用することで、にせものと判断することができるが、実際のプリンタで記録された場合には、偽物と判断することはかなりむずかしい。

このような場合には、以下のような対応が考えられる。例えば第５図(a)のＩＤカードの写真部の右上の４つの画点は特別な画点であり、例えば第５図(c)のような重みを持っているものとする。例えば第５図(c)のように2^0と2^3の位置に画点があるとすると、これは、９を表わしている。そこで第５図(b)で確認データを計算する場合に、更に画像の中に隠されている数字（この場合は９である）を、一緒に合わせて計算すれば良い。つまりＩＤカードのチェックを行う機械で、パーソナルデータと画像中に隠された数字（文字）を読み込み計算した結果が、確認データと一致しているか否かによってＩＤカードの真偽をチェックする。つまり写真画像を詳しく調べて、この中からチェック用のパターンを見つけることはかなり困難であるので、ＩＤカードを偽造が非常に困難となる。また、全画素を忠実に再現できる精巧なプリンタが必要となる。

なお第５図(c)のような方法を使用する場合には計算に用いるデータとしては第５図(d)のように画像中に隠されている数字だけでも充分である。極端な場合には変換もほとんどしないで、そのまま確認データとして出力しても良い。また確認データも、第５図(c)に示すような方式で表示してもよい。

◦第６の実施例

明らかに目に見える模様を写真の中に記録しておいたのでは、プリンタを使用することによって偽造されてしまう。偽造防止するためには、写真画像中に記録されている文字が

① 普通の光線状態では、人間は直接読めない。

② 暗号化された状態で記録されており、どこに、どのような状態で記録されているのか、他人には判別できなくする。

③ ①と②を合わせ、特殊な光線を使用することによって、写真部の中から、暗号化された文字を読み出す。

などの方式が考えられる。

まず最も簡単な方法としては、パーソナルデータ内にある文字あるいは数字から、特殊な計算式によって得られた文字列を、通常では、見えないインクで記録する方法である（第３図参照）。例えば紫外光をあてると、可視光を発生するようなけい光インクを使用することが考えられる。また、このように可視光を発生するものでは、ある場合には記録されていることがわかってしまう場合もある。そこで、特に秘密を厳守したい場合には、紫外光を与えると、赤外光のけい光を発するような、けい光インクを使用することが望ましい。このようにすることによって通常の状態では、写真部に書かれた文字を認識することはほとんど不可能である。つまり、紫外光を発生する装置と、赤外光を認識する装置を１つの筐体の中に持ったＩＤカードの読み取り装置によってその真偽の判定が可能となるわけである。

なお、この場合にも写真部に記録される数字あるいは文字は、数字・文字そのものでなく、ＡＳＣⅡなど、あるいは特別に作った文字コード，バーコードなどであった方が良い。文字のコード化も一種の暗号化であるが、更により積極的に暗号化を行なった方が理想的ではある。

◦第７の実施例

パーソナルデータを暗号化して顔写真の中に記録する方法の１例を示す。ＩＤカードの顔写真は、階調性と解像度を重視しているために、昇華性プリンタが使用されている。従って各画点は例えば１２８階調程度のパルス幅制御が行なわれており、１つの画点は１２８階調に制御される。そこで暗号化する方法としては、写真の中の一部分に、パーソナルデータから得られる文字・数字列を、各画点の濃度に置き換えて、（暗号化）し

て記録しておく方法が考えられる。しかしこの方法では、インクの経時変化や各階調間の濃度差があまりにも小さすぎることを考えると、採用するには、あまりにも無謀で、あほらしすぎて、何か考えているとは考えられない状況である。

暗号化するためには、画点があるか否かの2値の情報を使用するのが最適である。つまり、写真の中の一部分に、2値のパターンで、パーソナルデータあるいはその一部又は、パーソナルデータから作成される文字・数字などを暗号化して記録する方法である。例えば第6図(a)にその実施例の1つを示す。図のように写真の一部の斜めの部分にこのデータを記録するのである。このように、写真の一部に斜めにこのデータを記録しているのは、写真画像の外縁にこのデータを入れた場合には、このデータ部だけ残して写真部だけ入れ換えられることを防止するためである。

パーソナルデータと暗号化して、写真部の斜線領域に記録する方式について述べる。第6図(b)がその一例である。この図の4つの画点にはそれぞれの位置に応じて2^0，2^1，2^2，2^3の4つの重みが与えられている。このようなパターンをＩＤカードの写真中の斜線部に記録しておく。例えば2^1，2^3の位置だけが適当な濃度で記録されているとすると、$2^3\times1+2^2\times0+2^1\times1+2^0\times0=10$を表わしていることになる。また第6図(b)の斜線部で示される部分は、ダミーのビットであり、適当な濃度で記録されているとする。またデータの記録開始位置は、予め定められているので、この斜線部の決められた位置からデータを読み始めれば良い。あるいは、データを書き始めてあるというスタートコードを記録しておき、そこから確認用データが書き込まれているとなっていてもよい。以上のようにすることによって、ＩＤカードのパーソナルデータ又はその一部あるいは、これから生成されるデータを、写真部の一部に書き込むことができる。

なお、写真部は、Ｙ，Ｍ，Ｃの3色あるいはこれに更に黒を加えた、昇華性のインクで記録されることになる。第6図のように写真中に書き込まれたデータは、これらのインクのどれか1色を決めて記録しておけば良い。他のインクは全く無秩序に分散させることによって、第6図に示した様な斜めの確認データを書き込まれたラインが記録される。予め何色のインクで確認データを記録してあるのかを決めておく、あるいは、何色のデータが確認データであるかというデータをこのデータの中に書き込んでおく、又は各4画点毎に確認データを記録してあるインクの色を変えてゆくなどの方法を使用することによって、写真部に記録してある、確認データを読み取ることができる。そして、パーソナルデータ部を読み取った結果と比較することによって、このＩＤカードの真偽を判定することができることになる。

・第8の実施例

第7の実施例の別の実施例の1つとして、ＩＤカードの確認用のデータは通常の顔料を用いた熱溶融性のカラーインクで記録する方法がある。例えば、ＩＤカード確認用のデータをＭの顔料性の熱溶融性インクで記録する（第7図(a)）。そして更にこの上に今度は同じＭの染料性の熱昇華性インクで例えば第7′図(b)に示した様に、全面を斜線で塗ってしまう。つまり、このようにすることで、肉眼ではマゼンタの斜めのラインが確認できるだけである。ここでＩＤカードの読み取り機で赤外光を使用すると、染料インクに対して赤外光は透明である（第2図参照）ので、顔料インクが記録されて、斜線の下に隠されていたＩＤカード，確認用のデータだけを読み取ることが可能となる。

以上、幾つかのＩＤカードの真偽を判別する方式について示してきた。これらはいづれも読み取り装置を必要とする方法であり、チェックの段階によって、あるいは使用目的の重要度によって読み取り装置の大きさや構成も大きく異なる。最も重要な場所や、ＶＩＰ級の人間の集まるような場所へ入場する場合には、ここに示した全ての真偽判別法を行うことはもちろん、目視によるチェック等も充分に行なわなければならない。

しかし、通常はこのような厳重なチェックは必

要無く、簡単なチェックだけで充分である。例えば最も多い偽造としては、写真部に自分の写真を入れて偽造ＩＤカードを作る方法などが考えられる。このような場合には、本実施例の1および2程度のチェックでも充分に、チェック機能をはたすことが可能である。

第８図に最も簡単なＩＤカードの真偽判別装置を示す。この装置は、少なくとも赤外ＬＥＤアレイ(4)と赤外ＣＣＤアレイ(5)から構成されている。ＩＤカード(7)は例えば矢印Ａのような方向に動き、赤外ＬＥＤアレイ(4)から出た赤外光はＩＤカード(1)に反射した後、赤外ＣＣＤアレイ(5)へと入射する。文字部(3)は顔料インクで記録されているので赤外光は充分吸収されるので、赤外ＣＣＤ(5)には、文字部(3)に記録されている文字パターンが入力される。この時赤外ＣＣＤアレイ(5)の解像度を充分小さくしておくと、文字部(3)を記録したプリンタの解像度が、図示してはないが装置内の回路によって求められる。この文字プリンタの解像度が規定通りでない場合には、このＩＤカードは偽物と判定される。文字部が本物であると判定されたＩＤカード(1)は、更に矢印Ａの方向に移動され、写真部(2)が赤外ＬＥＤ(4)の下に来る。昇華性インクで記録された本物のＩＤカードであれば写真部(2)を走査した場合には、ＣＣＤアレイセンサ(5)には、赤外光がほとんど一様に反射して返ってくる。従ってこの場合には本物のＩＤカード(1)であると判定できる。写真部(2)を他人の写真等に入れ換えた場合にはＣＣＤアレイ(5)からの出力写真パターンによって変化するので偽物のＩＤカードであると、すぐにわかる。この方式によるＩＤカードの真偽判定法のフローチャートを図９に示す。なお、余裕のある場合には、読み込んだ文字部(3)のパーソナルデータを計算し、実施例の8に示した様な方法でこの計算値を予め写真部(2)の中へ隠しておき、これらのデータを読み込んだ時に再びチェックすることを行えばかなり高い精度で、ＩＤカードの真偽の判定ができる。

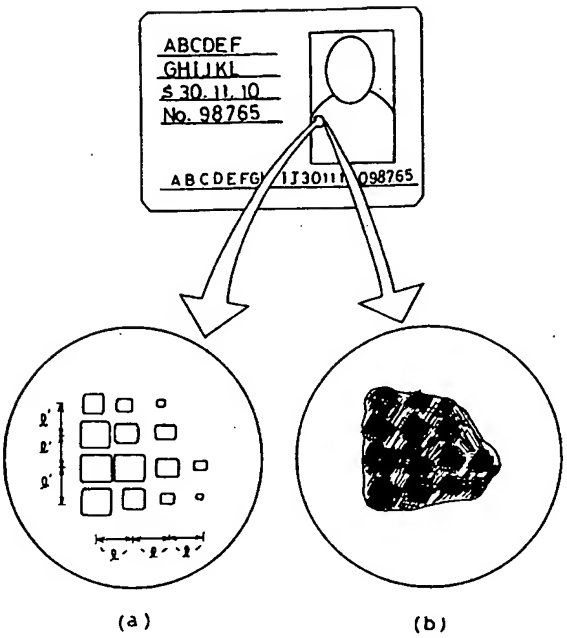
［発明の効果］

この発明を用いることにより、パーソナルデータと写真入りのＩＤカードの偽造を困難とし、もし偽造されたＩＤカードが作られたとしても、簡単に、偽物のＩＤカードであると判定できるＩＤカード判定装置を構成することが可能となる。

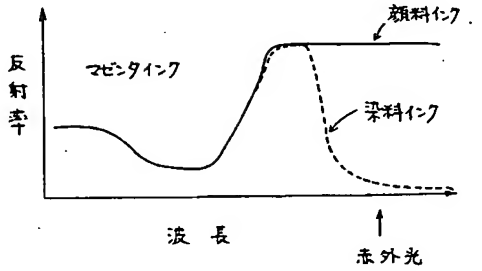
4．図面の簡単な説明

第１図は、ＩＤカードと、本発明の第１の実施例を説明するための図，第２図は染料インクと顔料インクの反射特性を説明するための図，第３図は、けい光インクを使用した場合の光の吸収と発光を説明した図，第４図は、ＩＤカードを２つの異なった解像度のプリンクで記録し、場所によって規定通りの大きさの解像度になっているか否かで、ＩＤカードの真偽を判別する方法を説明するための図，第５図はパーソナルデータを用いた計算から求めた、データを写真部分に記録しておき、ＩＤカードを読み込んでパーソナルデータを計算した値が、写真部分に記録されているデータと一致するか否かによってＩＤカードの真偽を判別する方法を示す図，第６図は、確認用のデータを写真部に記録する別の方法を示す図，第７図は熱溶融性インクでこのデータを記録し、更に染料である熱昇華性インクを使用して、肉眼ではこのデータを見えなくする方法を示す図，第８図は本発明のＩＤカード真偽判別装置の最も簡単な例を示す図，第９図はこのＩＤカード真偽判別装置のフローチャート，第１０図はＩＤカード(a)とその写真部だけを入れ換えた偽造ＩＤカード(b)の例を示す図である。

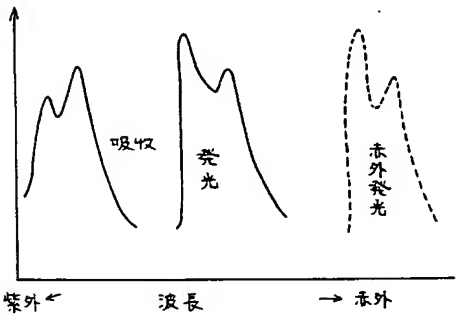
代理人弁理士　則近憲佑
同　　松山允之



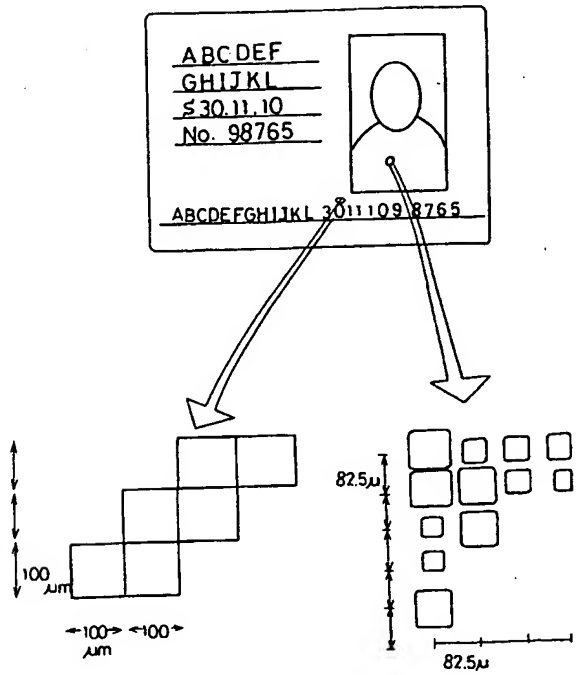
第 1 図



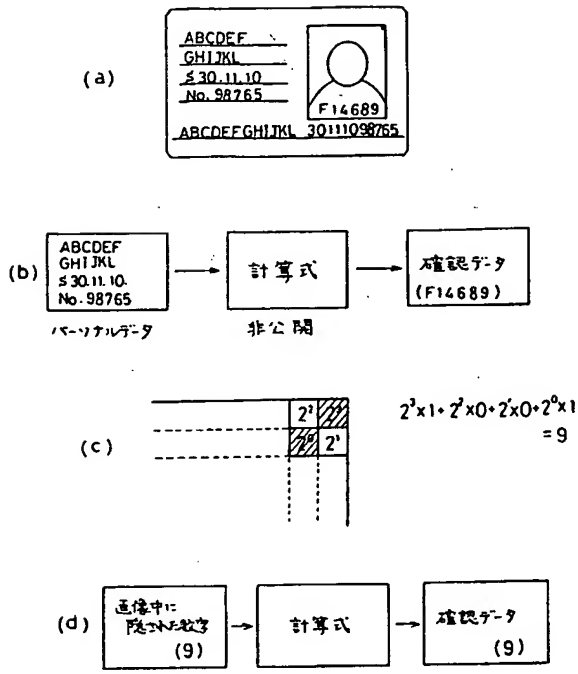
第 2 図



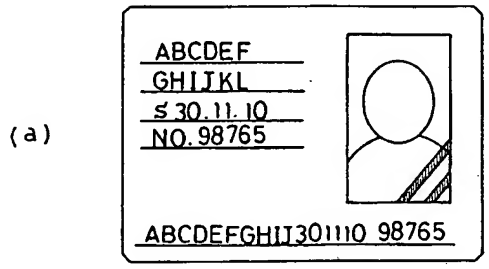
第 3 図

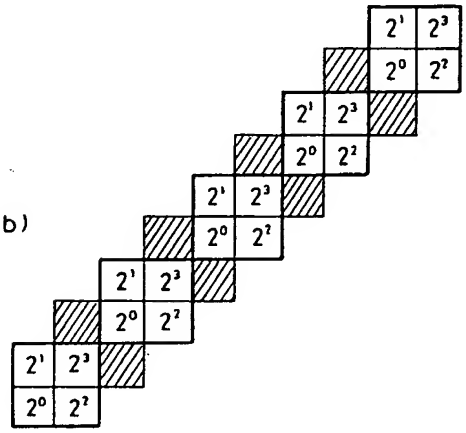


第 4 図

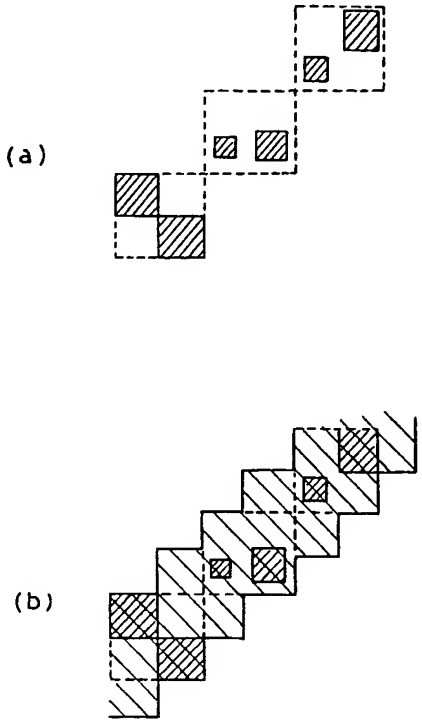


第 5 図

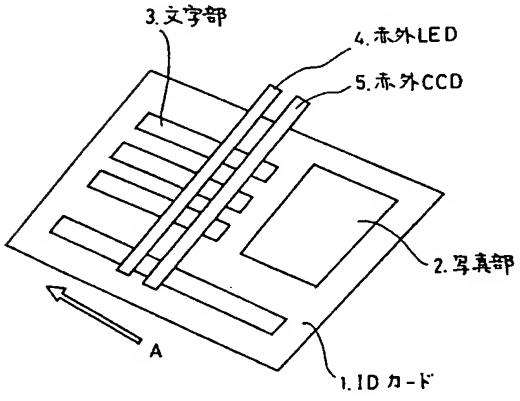




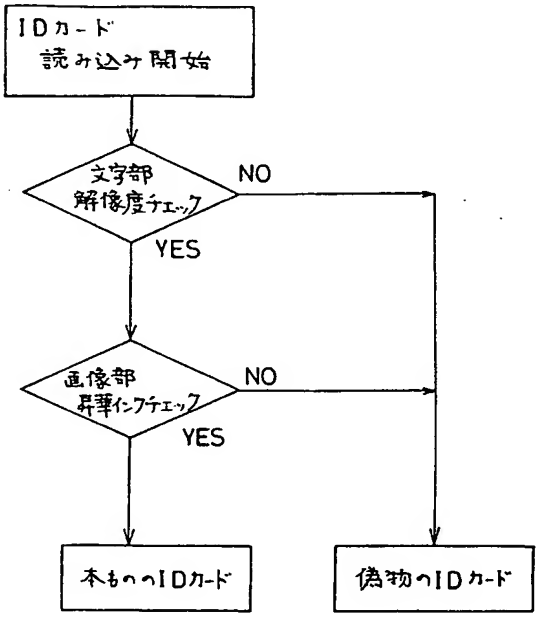
第 6 図



第 7 図

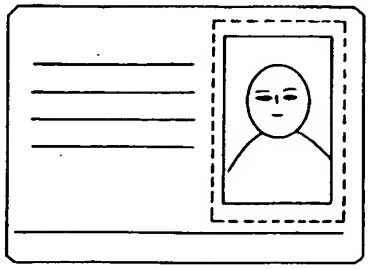


第 8 図

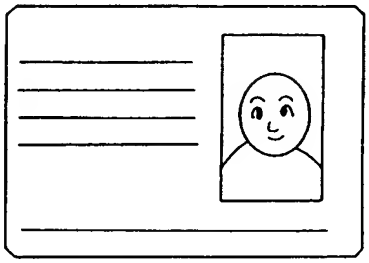


第 9 図

(a)



(b)



第 10 図